State of California

Child Welfare Services/Case Management System

CWS/CMS Exchange Architecture

March 31, 2004

Version 2.0

Table of Contents

1.0 Introduction 3

1.1. Exchange Architectural Requirements 3

2.0 Naming Conventions 4

2.1. Organization Name 4

2.2. Site Names 4

2.3. Server Names 4

2.4. Mailboxes 5

2.5. Distribution Lists 6

2.6. Custom Recipients 6

2.7. Connector Names 6

2.8. Monitor Names 6

2.9. Container Names 6

3.0 Directory 7

3.1. Directory Architecture 7

4.0 Information Store 8

4.1. Information Store Architecture 8

5.0 Connectivity 10

5.1. Intrasite Communication 10

5.2. Intersite Communication 10

5.3. External Internet SMTP mail 10

6.0 Exchange Client Configuration 11

6.1. Client Architecture 11

7.0 Scheduling 12

7.1. Implemented Architecture 12

8.0 User Administration 13

8.1. The Support Responsibility Structure 13
8.2. Server Administrative Responsibilities 13
8.3. User Support Responsibilities 15
8.4. Personnel Guidelines for Tier Support 19
8.5. Exchange Support Structure Needs 21
9.0 Backup 30
9.1. Backup Tape Rotation 30
9.2. Online vs. Off-line Backup 30
9.3. Local vs. Remote Backup/Restore 30
9.4. Location of Data Files 31
9.5. The Backup Process 31
10.0 Site Configuration 33
10.1. Central Exchange Counties 33
10.2. Central Exchange Counties versus Local Exchange Counties 34
11.0 NT Domain Architecture 35
11.1. Requirements 35
11.2. Architectural Design of the CWS/CMS NT Domain Model 35
Appendix A 36
Appendix B 46
Appendix C 47
Appendix D 49

1.0 Introduction

The purpose of this document is to provide an overview and analysis of the architecture for the implementation of Microsoft Exchange (Version 5.5). Its content is product specific and technical in nature. The goal is to provide the reader with an in-depth understanding of integral aspects of the network architecture of the implementation of this collaborative messaging product.

1.1. Exchange Architectural Requirements

Overall architectural requirements are based upon specific user and deployment requirements and the following assumed conditions:

- County sites with 10+ users will have T1 access to the HHSDC Frame Relay network
- On average only 1/3 of users on site will be actively using mail at any one time
- There is one high bandwidth (T1 circuits or faster) WAN entry points from the HHSDC Frame Relay network to Central Exchange server segment and/or segment router

1.1.1. User Requirements

The following user requirements have been identified to provide a basis for establishing the exchange architecture:

- *Ability to send messages to same recipient base.* Users must be able to send messages to the same recipients during and following the migration.
- *Ability to receive.* Users must be able to receive messages from the same users, both external and internal, following the migration.
- *Message delivery.* The speed of message delivery must be equal to or better than the Microsoft Mail system.
- *Data migration.* Existing messages and personal address books must be migrated to the new system.

1.1.2. Deployment Requirements

The requirements associated with deploying the product in a manner designed to be as disruptive to user functionality during user migration are identified as follows:

- *High volume of users per migration period.* To minimize the migration period, it must be possible to migrate hundreds of users at a time (evenings and weekends).
- *Post office name transparency.* To minimize addressing problems, it must be possible to transparently move an entire post office to Microsoft Exchange.

2.0 Naming Conventions

A key element in an effective Microsoft Exchange deployment is the development of a naming convention that meets simplified management goals and provides room for system growth. Outlined below is the naming convention deployed in the CWS/CMS environment.

2.1. Organization Name

This is the name of the organization in which Microsoft Exchange is being installed. The only significance to this name is that it cannot be changed without reinstalling Exchange Server, and one organization cannot connect to another Exchange organization if the names are different. The organization name is used to generate foreign e-mail addresses and the name of all directory objects such as mailboxes, public folders, and distribution lists. The organization name can contain up to 64 characters.

The Exchange Organization name for CWS/CMS is **CA**.

2.2. Site Names

Like the organization name, site names must be unique and cannot be changed. Sites can be given display names according to physical location.

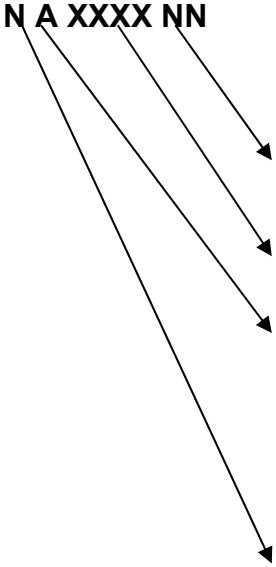
The CWS/CMS site name is **CWS-Central**.

2.3. Server Names

Microsoft Exchange uses the Windows NT Server computer name for the Exchange Server name. Server names must be unique and cannot be changed without reinstalling Exchange Server. With Exchange 5.5, there is a **<Server Location>** field, which can be used to describe the specific Exchange Server function. Additionally, a meaningful description for the server should be added using the Windows NT Server Manager utility.

Server names consist of eight characters in four fields as follows:

N A XXXX NN (Example – ND071501)



Character	Description
NN	A unique two digit number between “01” and “99” representing a specific Server
XXXX	The site ID code
A	This field is used to designate the Server Type as follows: D = Domain Controller B = Backup Domain Controller S = Additional Server
N	N is a constant representing an NT Server

2.4. Mailboxes

Mailbox names should be easy to identify and are based on the existing CWS/CMS naming standards for PC-based e-mail. The following fields can be specified in a mailbox name:

Field Name	Description
First Name	The user’s first name. Up to 64 characters in length.
Last Name	The user’s last name. Up to 64 characters in length.
Alias Name	The Mailbox Alias Name will be the user’s <last name (5)>, <first initial (1)>. If there is a duplicate Alias Name, resolution would be provided through the RACF (CWS/CMS Application) user ID. The Alias Name is limited to seven characters.
Display Name	The user's Display Name is <last name>, <first name>.
Proxy Addresses	The user's Proxy Addresses include the following SMTP proxy: <*Alias Name*>*@cws.state.ca.us*

2.5. Distribution Lists

Distribution Lists have descriptive names, are not case-sensitive, and should not use any special characters. Distribution List names will not be prefaced by any special characters, as they are preceded by a **Distribution List** icon in the GAL (Global Address List). Ownership and maintenance of these lists can be assigned to users.

2.6. Custom Recipients

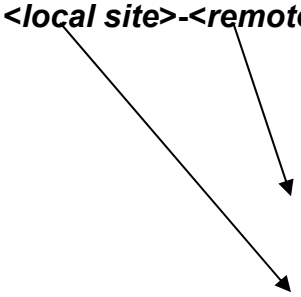
The **CA** site will maintain all custom recipients, both non-Exchange CWS staff and aliases for addresses outside of the *cws.state.ca.us* domain.

2.7. Connector Names

The display name for the connector (up to 256 alphanumeric characters) should include the names of both the local and remote sites it connects. The display name should be defined the same as the directory name.

The directory name for the connector should be defined as follows:

<local site>-<remote site> (Example – CWS-Central-Kings)



Site Directory Identification	Description
<remote site>	The directory name used for the remote Exchange site.
<local site>	The directory name used for the local Exchange site.

2.8. Monitor Names

The display name for link and server monitors should be descriptive, use standard sentence syntax, and include an explanation of the monitor's purpose. The directory name should be short and include a description of the monitor type.

2.9. Container Names

Since containers and their contents are visible across the enterprise (listed below each site in the address book), they should be carefully created and have descriptive names. The standard **RECIPIENTS** container should not be used. Each county will have its own recipients container.

3.0 Directory

The Directory is one of the most important components of Microsoft Exchange. It stores all relevant information regarding the users of Exchange and those that can be reached via Exchange. In addition, the directory stores all of the configuration information from all the other components.

To make the information accessible to users and Exchange components, the Directory Store is replicated across the Exchange organization. Within a site, all Exchange servers exchange all their directory information with each other automatically.

3.1. Directory Architecture

Below are specific recommendations regarding the configuration and implementation of the Exchange directory.

3.1.1. Administrative Changes

To minimize traffic and improve the distribution of directory changes, make directory changes on the bridgehead server of the site. This will allow changes to move immediately to other servers at the site. In addition, always make directory changes at the same server in the site to reduce the possibility of replication conflicts within the site.

3.1.2. Synchronize Changes Only

Implement processes so that only changes in data are received from external sources, rather than all of the data. This will minimize traffic on the network and ensure that the directory is replicated in a timely fashion.

3.1.3. Utilize NT Security Groups

To ensure the accuracy of the data that is contained in the directory, restrictions should be placed on who can modify portions of the Exchange Directory. This is best implemented by establishing NT security groups and assigning Exchange permissions to that group.

3.1.4. Minimize Use of Recipient Containers

Users of Microsoft Exchange can be divided into several types and placed into recipient containers. Minimize the use of recipient containers because it is difficult to move users from one recipient container to another. Special containers are used to store special objects such as Enterprise distribution lists and foreign custom receipts. This enables selective export of special objects to Exchange. This also helps users looking up these special objects in the address book. Each county has only one recipient container.

4.0 Information Store

The Microsoft Exchange information store is responsible for storing, retrieving, and managing user data. Although transparent to the end user, the Exchange Server information store consists of two databases or message stores. These are referred to as the private and public stores. The private store consists primarily of user message data and mailbox rules; the public store consists of public folder data and electronic forms applications.

The Exchange information store supports online backup, online defragmentation, and Mailbox storage limits. Online backup allows the information store to be backed up without interrupting Exchange messaging services. End users can connect and have full functionality during the information store backup process. Administrators can restrict the amount of data the end users can store in the information store.

4.1. Information Store Architecture

Below are some specific recommendations regarding the configuration of the Exchange information store.

4.1.1. Use Server-Based Mailboxes

One of the CWS/CMS user business requirements is that users need to be able to access their e-mail through multiple workstations at different locations. To meet this objective, all CWS/CMS users will use the server-based mailbox as their primary e-mail storage. This will allow them access to their inbox from any network-connected desktop machine. By using a server-based mailbox, users will get the same view of their mailbox no matter which desktop they use to access it. Another benefit of using a server-based mailbox is that it allows Exchange Administrators to backup users' mailboxes on a centrally-controlled tape without interruption to user e-mail access.

4.1.2. Mailbox Size Limits

Due to limited disk space on the Exchange servers, it is necessary to configure personal mailbox storage limits and a maximum age on server-based messages in public folders. Based on Exchange server disk space, the recommended mailbox storage limit is 40 MB. The user will receive a warning message and will be unable to send e-mail if their mailbox exceeds 50 MB.

4.1.3. Dedicated Public Folder Server

A dedicated public folder server enhances performance since the user mailboxes and related activity will occur on other servers. This function-based server design strategy allows for easier capacity expansion in the future.

4.1.4. Disable Circular Logging

Circular logging saves disk space but does not maintain a continuous history of transactions. Therefore, to enhance the recoverability of the information store, circular logging is not enabled.

4.1.5. Transaction Log

For maximum performance, transaction logs should be maintained on a RAID 5 partition. RAID 5 will balance the disk I/O among multiple RAID drives and will improve the performance of the Exchange information store. If the transaction logs share a drive with the NT swap file, disk I/O contention can occur and delay information store I/O requests. (See the server diagrams in *Appendix A* for detailed Exchange configuration information.)

4.1.6. Monitor Information Store

Information Store growth and performance is monitored periodically through NT disk space alerts. These alerts are setup to monitor remaining disk space.

5.0 Connectivity

Messaging connectors and Directory replication connectors are required for an Enterprise Exchange Messaging environment. Message connectors are the primary method of intersite communication. All intersite message communication will take place via a messaging connector. Directory replication between sites also depends upon the underlying existence of a messaging connector. There are four standard types of message connectors; however, the State of California only relies on two types of connectors for internal messaging communication and one connector for external communication.

5.1. Intrasite Communication

Normally servers within a site communicate directly through the Message Transfer Agent in order to exchange messages from one Directory Structure (DS) to another to exchange directory information. Within a site, directory replication is able to take place via direct DS to DS communication.

5.2. Intersite Communication

The connectivity described above is not directly possible for communication between sites. Therefore, a "connector" must be used to establish a logical transport link between sites. These connectors rely on the presence of a physical high-speed connection between sites. To establish communications between sites (e.g., Alameda, Contra, San Diego, and Ventura) SOC CWS Exchange uses four named SITE messaging connectors and four named directory replication connectors.

Directory Replication Connectors allow sites to share directory information and it takes place over the Directory Replication connector via Site connectors. Directory Replication connectors rely on existence of messaging connectors which in this case are the 4 site connectors mentioned above.

5.3. External Internet SMTP mail

The Internet Mail Service provides the ability to handle Simple Mail Transport Protocol (SMTP) mail. SMTP is the protocol used on the Internet to transfer messages. Using DNS supported by HHSDC, messages are transferred over the Internet to external hosts. The IMS also accepts inbound messages coming from the Symantec SMTP Gateway after being scanned for malicious content.

6.0 Exchange Client Configuration

Depending on the type of client access, users in the CWS/CMS network environment can be classified into two groups:

- Desktop Users: These users have an Exchange client on their desktop. Some of them need to use different computers to access their Exchange mailbox.
- Mobile Users. These users carry their laptops with them or use a workstation other than a CWS/CMS workstation and need access to their mail from different locations. They use the same machine for access, but could use an asynchronous connection or the network to connect.

6.1. Client Architecture

Client architecture depends upon whether the user accesses their mailbox directly from their workstation on the network or remotely via a dial-in method.

6.1.1. Message Storage

All users use the server-based mailbox as their primary storage. Users of Outlook can also use personal folders on their desktop or a server as a message archive. Remote users should use an Off-line Folder Storage (OST) file. Offline folders make it possible to take a folder from a server location, work with the contents of the folder when not connected to the network, and then update the corresponding server folder with any changes. This allows the users to access both private and public folders while they are off-line. Users' inbox and outbox folders are automatically synchronized when the client logs in. Users can also synchronize other folders by simply choosing the synchronization option from the menu list when they are online.

6.1.2. Remote Strategy

Microsoft Exchange allows clients to access their mailbox and public folders remotely, through the dial-in connection available as a function of the dial-up architecture.

6.1.3. Remote Dial-In

All remote Exchange users need some form of PPP (point-to-point protocol) connectivity to make a connection to their Exchange server. This conductivity is provided by AT&T Network, and as long as they have remote network access to the CWS/CMS network, their Exchange server mail access will be very similar to when they are directly connected to the network.

7.0 Scheduling

Microsoft Exchange supports the use of the calendaring features available in Outlook. The scheduling architecture is currently not deemed a business requirement and is not implemented. The Exchange server architecture reflects only e-mail traffic requirements. In the future, if scheduling is required, a solid NT and Exchange infrastructure will be in place to support scheduling. The following sections are provided in the event that the Project elects to implement the use of scheduling.

The Outlook Calendar module combines the functionality of Schedule+, plus additional features, with the GroupWare capabilities of Outlook. When located in the Mailbox or Personal Folder, the Calendar module enables users to create personal schedules, create reminders, or set up meetings. When the Calendar module is copied to the Exchange Server, however, it can be used for sharing group schedules. (e.g., posting the significant events in a release kickoff, making a class schedule publicly available, or posting holidays in a public folder).

7.1. Implemented Architecture

7.1.1. Free/Busy Information

When the first server in a site is installed, Exchange automatically creates a hidden public folder per site that contains each user's Free/Busy information. This server will be the public folder server and will process requests for user Free/Busy information, and maintain that information for distribution to all users who request it through Schedule+.

7.1.2. Calendar Shared Resources

All shared resources, such as conference rooms, should be represented in the Exchange directory. All users will have read access to these shared resources. Scheduling will be done through a designated shared resource administrator. For example, there can be a container called Conference Rooms. This container would have a sub-container for every building that has conference rooms. The conference rooms' calendars would be placed in these location containers.

7.1.3. Schedule Synchronization Interval

Outlook's calendar keeps each user's schedule information in the user's mailbox. Outlook synchronizes users' schedule information with the free/busy folder stored on the public folder server. The synchronization interval between user calendars and the free/busy folder is 15 minutes.

8.0 User Administration

This section provides an overview of an Administration Plan for CWS/CMS Exchange Servers, including:

- A description of the support group structure including the roles and responsibilities of the three tiers within the group
- A description of the expected personnel qualifications for each level of tier support
- A definition of the Exchange support structure that needs to be in place to support the entire Exchange Server infrastructure for CWS/CMS Exchange End Users

8.1. The Support Responsibility Structure

Exchange support responsibilities fall generally into two separate categories. The first is administrative in nature and involves the management of Windows NT Exchange Servers. The second category relates to user support. These categories involve the use of tiered levels of support, and the nature of a problem is used to identify the support tier responsible for problem resolution.

8.2. Server Administrative Responsibilities

Identification of the major areas of responsibility associated with the administration and support of Exchange servers, and a brief description of each responsibility, are listed below.

Organization	Responsibility	Description
County/State	Windows NT User Accounts	User account established on a Windows NT Server Primary Domain Controller.
NWS	Windows NT Global Group	Global Group account established on a Windows NT Server Primary Domain Controller. Global Groups are composed of individual users and can be used to facilitate user access to resources located in another domain (referred to as the trusting domain).
NWS	Windows NT Local Group	Local Groups are accounts established on Windows NT Servers and Workstations. Local Group members can be either Users or Global Groups and are customarily used to define who can access resources on an NT Server or Workstation.
NWS	Windows NT Trust Relationship	NT trust relationship allows cross-domain administration and resource access. The NT trust relationship is composed of two or more domains, where the “trusting” domain allows access (including administration of) its resources by users in the “trusted” domain(s).

Organization	Responsibility	Description
County/State	Exchange User Account	This User Account is separate and distinct from a NT User account. It establishes a user account on an Exchange Server, providing a location for the receipt of e-mail and other collaborative mailing features.
County/State	Exchange Public Folders	These root-level folders, located on an Exchange Server, are provided for storage and distribution of files to Exchange Users. A key benefit of public folders functionality is it allows users to share information.
County/State	Exchange Distribution List	Similar in nature to Windows NT groups, an Exchange Distribution list identifies a list of recipients on an e-mail list. It can include Exchange users and groups identified collectively for the purpose of delivery as a single mail recipient.
NWS	Exchange Site Connection and Replication	This process involves establishing and maintaining communication links between Exchange Servers in a single “exchange server farm.” The replication of information is necessary to insure that users can access their e-mail in a multi Exchange Server environment.
NWS	Exchange Directory Synchronization (with other messaging systems)	This process involves the configuration of Exchange Servers with other messaging systems so users can interact and exchange e-mail.
NWS	Exchange Internet Mail Connection	This process involves the maintenance of the Exchange Server’s mail connection to the Internet, so mail can be distributed to others using the Internet as the communications path, and e-mail addressed to an Exchange user and sent across the Internet will make its way to the User’s Exchange mailbox.
NWS	Exchange Server Monitoring	This process involves monitoring an Exchange Server to determine if it is properly processing information and requests. The process also involves preventative analysis, designed to ascertain whether system upgrades are necessary.
NWS	Exchange Server Maintenance	Exchange Server Maintenance includes periodic maintenance activities associated with performance tuning, including hard disk maintenance and other tuning activities.

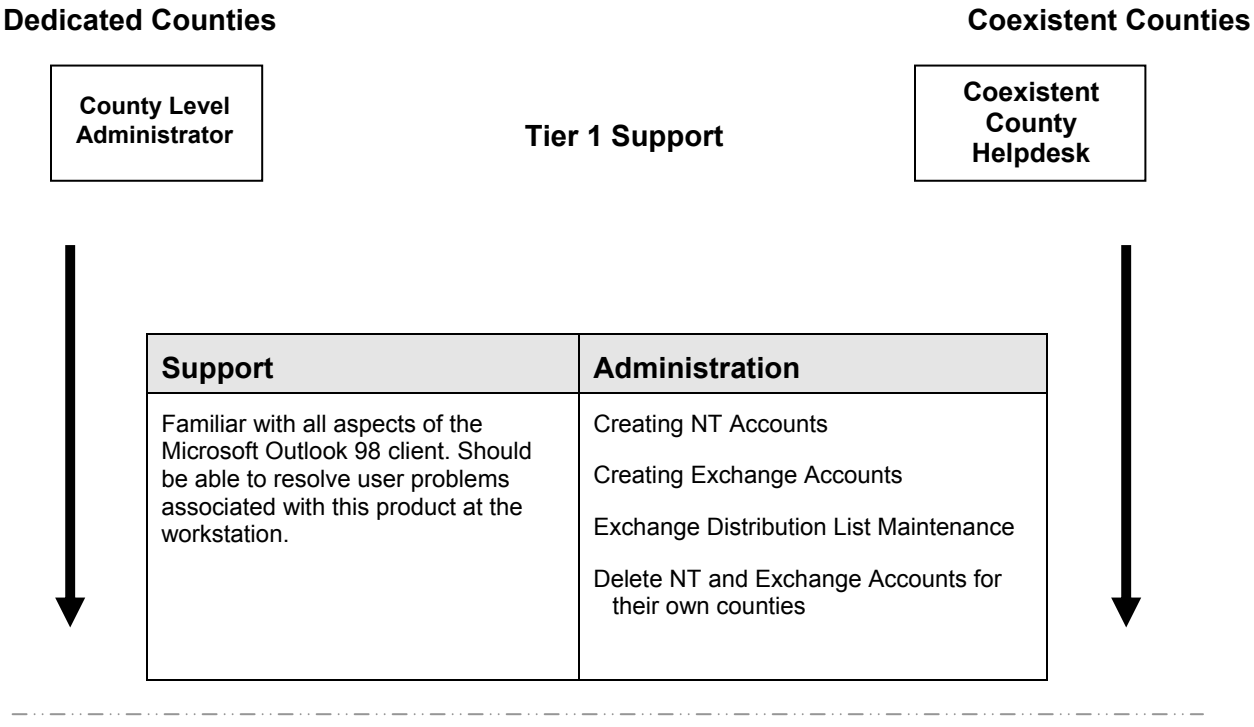
Organization	Responsibility	Description
NWS	System Upgrade	System upgrades fall within two categories: The first involves the replacement of existing hardware that is designed to improve overall system performance. The second relates to software upgrades, including the installation of service packs designed to repair software problems, provide added functionality, or improve performance.

8.3. User Support Responsibilities

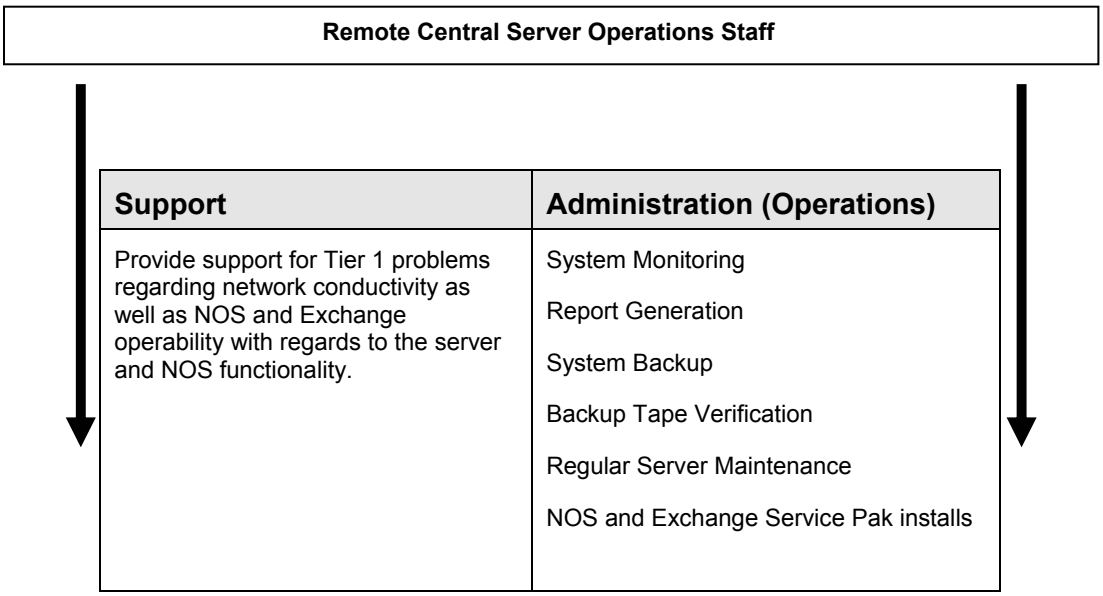
For purposes of defining User Support Responsibilities, the CWS/CMS Project has adopted a "tier" level structure. In this arrangement, the nature of a user's problem determines which level (tier) is responsible for problem resolution. This structure is similar for both dedicated and coexistent counties.

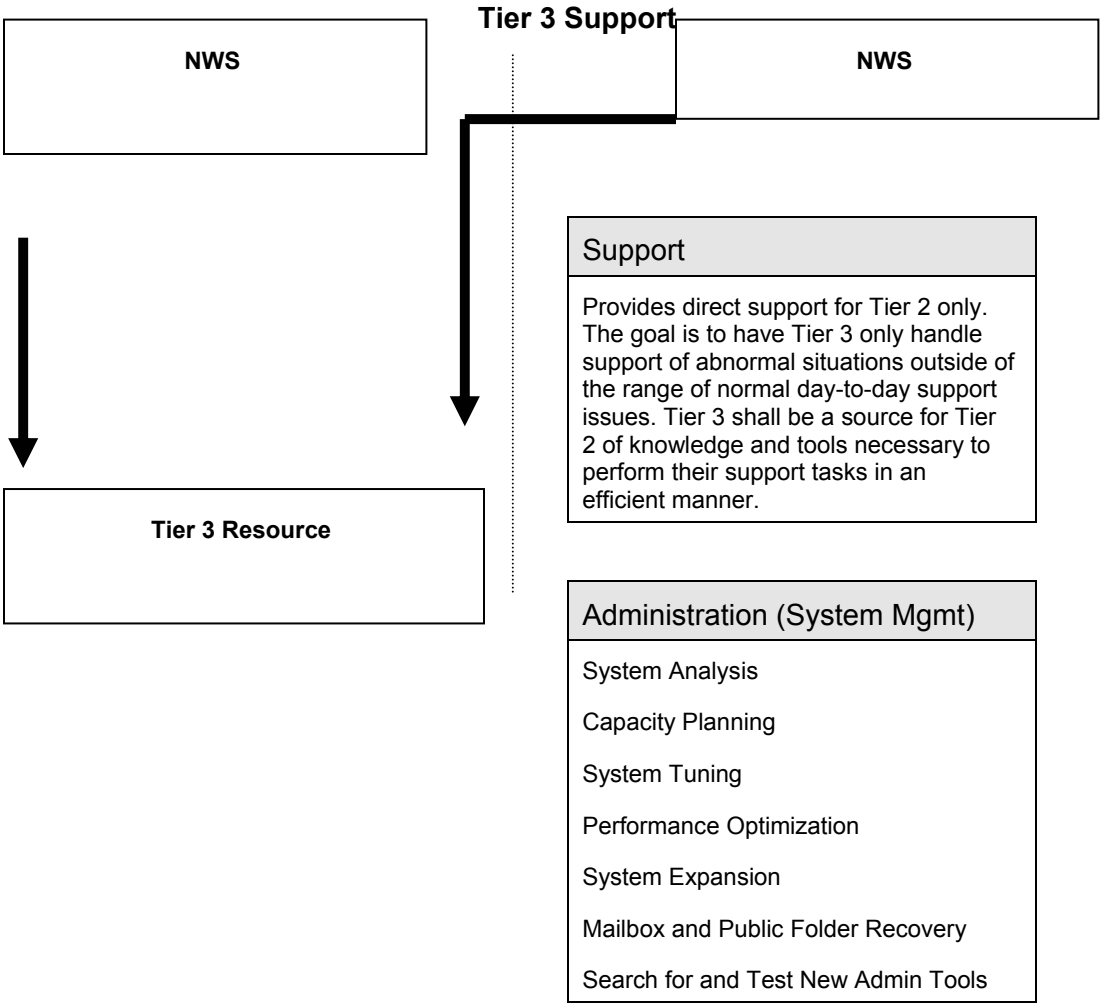
8.3.1. Tier Support Escalation Procedures

The figure below provides a visual representation of this "tier" structure, including a general description of the problems expected to be resolved at each level.



Tier 2 Support





The tier strategy is designed so that less complicated help desk issues and administrative functions are expeditiously remedied at a local level. More complicated problems are first passed up from the Tier 1 support level to Tier 2. If the Tier 2 personnel are unable to resolve the problem, they will seek Tier 3 support. This ensures that critical knowledge is transferred to Tier 2 to help resolve similar problems in the future, and it serves as on-the-job training that helps Tier 2 to resolve future problems and decrease dependency on Tier 3.

The goal is to have Tier 3 handle support for situations outside of the range of normal day-to-day issues. Tier 3 is a source for Tier 2 to gather the knowledge and tools necessary to perform their support tasks in an efficient manner.

Tier 3 performs all administrative tasks not defined to be performed by Tier 1 or 2 support levels. Tier 3 support is provided by the NWS Support Team, and the Tier 2 support staff is responsible for determining whether escalated problems need to be directed to Tier 3.

When an escalated problem is misdirected by Tier 2 support staff, rather than referring the matter back to Tier 2 support staff for redirection, a direct referral is made by the Tier 3 support component receiving the trouble ticket.

8.3.2. Tier 1 Support Escalation Procedures

As mentioned above, the goal is to obtain problem resolution at this level whenever possible. The key to handling matters at this level is the amount of Outlook 98 training Tier 1 support personnel have. Another key to effective resolution is the ability of Tier 1 support personnel to determine whether the problem should be resolved at their level or escalated to Tier 2 for support. If they decide that the responsibility for the problem's resolution rests with Tier 2 (usually an Exchange Server-based problem), it is immediately directed to Tier 2 for resolution.

If Tier 1 support personnel are unable to resolve a problem relating to the Outlook 98 client or other areas of designated responsibility, it should be escalated to Tier 2 for resolution or distribution to Tier 3.

8.3.3. Tier 2 Support Escalation Procedures

Tier 2 personnel are divided into two separate areas. Each is identified below, together with a description of their areas of responsibility.

Identity	Responsibilities
CWS/CMS Help Desk	This Tier 2 support group has responsibility for receiving the call from Tier 1 support and entering all required information into the Problem Management system. Initial problem determination identifies if the ticket should be referred to the NWS Support Team.
NWS Support Team	This Tier 2 support group has the responsibility for the management, maintenance, and availability of the Windows NT operating systems that support the Exchange Server.

As described above, support calls received by Tier 2 support personnel are initiated by Tier 1 support personnel. When a call is received by Tier 2, Problem Management software is used to provide a central database that includes the nature of the problem and a description of how the problem was resolved. Also included is key tracking information such as the person placing the support request, the date and time of the request, and support personnel assigned to resolve the problem.

Problem Management software is used to maintain a dynamic knowledge database of problems and resolutions. This database serves as a reference tool for support personnel and provides a resource for efficient and effective resolution of similar problems.

During normal problem resolution, Tier 2 works with other support groups. A key responsibility of Tier 2 support personnel is narrowing problem identification so they can resolve it or escalate it to the appropriate Tier 3 support level personnel.

In addition to resolving problems, Tier 2 support personnel have the responsibility of determining whether the problem is Outlook 98 client-based. If it is, Tier 2 support personnel

escalate the problem to the Tier 3 NWS Support Team for resolution. If Tier 2 support personnel determine that the problem is Exchange Server-related, efforts are made by Tier 2 support to resolve the problem. If they cannot, then the problem is escalated to the Tier 3 NWS Support Team.

8.3.4. Tier 3 Support Procedures

References to the Tier 3 support level fall into two categories. The first are cases where the problems are the type designated to be handled by Tier 3 personnel, such as Exchange Server capacity planning, performance optimization, and mailbox recovery.

The second category are problem cases that should have probably been handled by Tier 1 or Tier 2 personnel, but are escalated because of an improper diagnosis or inadequate training of Tier 1 or Tier 2 personnel.

Tier 3 personnel are identified below, together with a description of their areas of responsibility.

Identity	Responsibilities
NWS Support Team	This Tier 3 support group has the responsibility for Exchange Server management and maintenance.

Tier 3 support personnel can use a variety of outside resources to resolve difficult problems, including Microsoft's Product Support Services (PSS) Group.

8.4. Personnel Guidelines for Tier Support

The guidelines for Tier 1, 2, and 3 support personnel are identified below. These guidelines include specific examples of duties support personnel should be able to perform.

8.4.1. Personnel Guidelines - Tier 1

To be effective in their role, the following guidelines have been established for Tier 1 support personnel:

- Familiarity with problems Outlook users are likely to encounter when using the product
- Understanding of how to complete a fresh installation of the Outlook product, and how to:
  - Import information from a file or a personal folder file (.pst)
  - Export items to a file or to a personal folder file (.pst)
- Ability to troubleshoot the following items or components of Outlook 98:
  - add-ins, appointments, archiving, AutoCreate, categories, contracts, creating items, email, email editor, journal entries, linking and embedding objects, mail, mail merge, meetings, menu customization, sending and receiving messages, tasks, toolbar customization, and views
- Ability to create NT Accounts

- Ability to create Exchange Accounts
- Ability to handle Exchange Distribution List Maintenance
- Ability to delete NT and Exchange Accounts for their own counties

8.4.2. Personnel Guidelines Tier 2

To be effective in their role, the following personnel guidelines have been established for Tier 2 support personnel:

CWS/CMS Help Desk

- Experience in supporting Windows 95 and Windows 2000 desktop operating systems
- Experience with installation and use of the Outlook 98 client. Emphasis should be placed on the mail component, as it is the only supported component.

NWS Support Team

- Experience with Windows NT Server operation systems: Windows NT Server 4.0
- Experience in supporting Windows 95 and Windows 2000 desktop operating systems
- Experience with TCP/IP and NetBEUI
- Experience supporting and troubleshooting a LAN and WAN environment
- Experience with the installation and use of the Outlook 98 client in the Exchange environment
- Experience administering Microsoft Exchange and Windows NT

8.4.3. Personnel Guidelines Tier 3 – NWS Support Team

NWS Support Team personnel are expected to have developed an expertise with the Windows NT operating system and related BackOffice products. NWS support personnel designated to support the Exchange Server environment are also expected to have developed the skills associated with the installation, configuration, and maintenance of Exchange Server, including the following:

- Choosing a client installation and integration strategy
- Developing long-term administration strategies
- Developing security strategies
- Configuring Exchange Server for message recipients
- Importing directory and messages from other mail systems
- Installing and configuring Exchange Server clients
- Configuring address lists and accounts using the Administrator Program
- Configuring message tracking

- Configuring server locations
- Configuring Microsoft Windows NT security integration
- Managing site security
- Managing users
- Managing distribution lists
- Managing the directory
- Managing Private Information Stores
- Backing up and restoring Exchange Server

8.5. Exchange Support Structure Needs

This section focuses on support structure needs for Exchange Server. Most of this support responsibility falls on Tier 2 support staff personnel. Listed below are the requisite tools needed to provide this support, along with a brief description of what Tier 2 support personnel are expected to handle.

8.5.1. Required Resources and Desktop Applications

Several applications must be available to the Tier 2 team members so they can perform their assigned tasks. The table below identifies them and contains a brief description of their use.

Department	Management Application	Purpose
NWS	NT Server Manager	To administer the NT domain from NT Workstation
County/State	Domain Enterprise Administrator (DEA)[1]	To administer NT user accounts from Windows 95 and Windows 2000 workstations
County/State	Domain Enterprise Administrator (DEA)	Exchange mailbox maintenance
HD/County/State	Exchange Client and Outlook	Duplicate caller actions; access Exchange Client Online Help

[1] The Domain Enterprise Administrator (DEA) is described in detail in the user documentation for Domain Enterprise Administrator Version 1.51.

HD	TCP/IP Utilities	Network troubleshooting: PING
HD	Problem Management System	Logging of calls, via Call Tickets. Used for lookup of previous similar problem and the solution.

8.5.2. Exchange Server Support Functions

8.5.2.1. Windows NT Administration

Tier 2 personnel will perform occasional administrative tasks on NT. These tasks consist mostly of NT account creation and maintenance, as well as assigning group memberships, granting file system permissions, and clearing the event logs.

The Windows NT event logs, system, security, and application need to be saved and cleared at regular intervals. These logs contain information important for troubleshooting and performing system analysis, and they must be stored for at least three months.

8.5.2.2. Exchange Administration

The Exchange Server Administrator program is used to administer the services and components of the messaging system, view and manipulate the structure of the organization, and perform a variety of administrative tasks. Exchange Administrator is usually installed on the Exchange server or can be installed on the administrator's NT workstation. This allows for administration of the entire Exchange topology from the administrator's desk.

The following table describes Exchange administrative responsibilities associated with Exchange Mailboxes.

Department	Responsibility	Description
County/State	Mailbox Administration	Mailboxes are the containers for receiving and sending mail for a recipient. Usually, there will be one mailbox associated with each user. There may be special mailboxes shared by a group of users, for example, a common Help Desk mailbox. Mailboxes need to be monitored for activity and size.
County/State	Mailbox Creation	Mailboxes are created when the user's NT account is created. For a user that already has an NT account, an Exchange mailbox can be created via the Exchange Administrator's Program.

Department	Responsibility	Description
County/State	Mailbox Removal	If an Exchange mailbox does not show any activity within a specified time, the mailbox owner is contacted to determine if the mailbox should be retained. If the owner is unavailable (e.g., the user is on a leave of absence), the owner's supervisor is contacted to obtain the status of the owner. The last access date for a mailbox can be viewed from Exchange Administrator in Private Information Store Mailbox resources.
County/State	Mailbox Maintenance	The properly authorized county-level personnel can perform simple mailbox maintenance, such as name changes, adds to distribution lists, and corrections of proxy addresses. More complex tasks need to be performed by Tier 2 administrators and include alias and Proxy address changes, advanced property changes such as changing the storage limit available to the user, changing the server housing the mailbox, and mailbox relocation to other sites.
County/State/ NWS	Storage Limits	Users exceeding the allocated storage limit are unable to send e-mail (although they continue to receive e-mail). The size of these mailboxes must be reduced to below the allocated limit before the user can resume sending e-mail. Users requesting an increase of the available online storage from the default will be considered on an individual basis. If the request has a legitimate business reason, it is granted.
County/State/ NWS	Advanced User Permissions	Users can be granted permission to mailboxes other than their own, allowing them to access that mailbox as if they owned it. This may be required if users share a common mailbox, or when users are on leave and another user requires access.
NWS	Mailbox Relocation	For load balancing purposes, a mailbox may need to be relocated to another server within the same site or to a different site.
NWS	Relocation Within The Same Site	In this case, simply changing the Home Server field in the Advanced User Property page to the new server will automatically move the mailbox to the new server. No other action is required.
NWS	Relocation To a Different Site	Moving a mailbox into a different site cannot be accomplished by simply changing the home server. If a user relocates and needs the Exchange mailbox set up in another site, the mailbox will need to be exported and then imported.

The following table details the responsibilities associated with the creation and maintenance of public folders and distribution lists.

Department	Responsibility	Description
County/State/ NWS	Policies and Standards	Mailboxes are the containers for receiving and sending e-mail for a recipient. Usually, there will be one mailbox associated with each user. There may be special mailboxes shared by a group of users, for example, a common Help Desk mailbox. Mailboxes will need to be monitored for activity as well as size. The top-level public folder structure and ownership have been established. Any new top-level folder requests should be submitted to the top-level administration group for consideration. Workgroup folder requests should be directed to the respective owner of the top-level folder, who will create the folder and assign appropriate permissions. These folders will reside on the same server as the user(s) requiring access to the folder, and will not commonly be replicated. The folder description field will describe the folder's purpose and contents.
County/State	Replication	The top-level folders have been created. Top-Level administration group will determine replication of these folders, on a CWS/CMS countywide basis. Workgroup folders are created on the server where the majority of users requiring access to the folder are located, or on a public folder server in the site, if one exists. Workgroup folders will not be replicated. Should users on other sites require access to these folders, folder affinity can be used to allow these few users to connect. This mechanism will allow availability of workgroup folders for geographically dispersed workgroups to share information, without the need to maintain several replicas.

Department	Responsibility	Description
County/State	Public Folder Maintenance	To prevent public folders from growing uncontrolled, the content should be reviewed periodically and outdated material deleted from the folder. Upon creation of the public folder, there will either be a size or time limitation assigned to that folder. The owner will be prompted by support personnel to determine which limitation will be assigned. Owners of large workgroup folders should be contacted periodically and reminded to remove outdated materials from their folders. The CWS/CMS project does not allow public folders or workgroup folders to be replicated across the HHSDC Wide Area Network.
County/State	Distribution Lists	All Distribution Lists (DLs) created will be visible in the global address list (GAL). There is currently no provision for making certain distribution lists available only to local or site users. To prevent the creation of duplicate names for DLs, all DLs will be created and maintained in a central container. The ownership of the DL will be assigned to a user, who will maintain the membership of the DL. All requests for changes should be directed to the owner of the DL.

The table below focuses on the responsibilities associated with the general maintenance of the Exchange Server and associated components.

Department	Responsibility	Description
NWS	General Maintenance	The messaging infrastructure will be managed and supervised by a group of people who have the privileges to modify the contents of the Microsoft Exchange directory. This is different from a shared file system-based e-mail system, where individual e-mail servers are administered by local administrators. With CWS/CMS's Exchange, the entire messaging system will be administered centrally by the Tier 2 personnel. Exchange has been designed to perform housekeeping and maintenance functions in the background, while Exchange is running. However, there are times when manually performing these functions is beneficial, such as after a large change to the system or to re-synchronize a server directory after a long server absence. The regular Microsoft Exchange Server maintenance consists of periodically verifying the following actions: • The Message Transfer Agent (MTA), connectors, and gateways are transferring messages correctly and in a reasonable amount of time. • The information store is working properly and providing adequate resources and performance to users. • The directory is working correctly, and directory replication and synchronization are sharing the correct information. • A recent backup for each server's directory and information store is completed.
NWS	Maintenance for Exchange Message Transfer Agent	There are specific procedures on maintaining the Exchange server stores (IS and DS) as well as the Message Transfer Agent.

Department	Responsibility	Description
NWS	Message Transfer Agent (MTA) Maintenance	There is one Message Transfer Agent per Exchange server, responsible for delivering messages destined to other servers. The messages are put into the MTA queue, where they await delivery by the MTA. There is no periodic maintenance needed for the MTA.
NWS	Rebuilding the Routing Table	The MTA routing table is rebuilt automatically once per day, or when changes are made to the address space on a Connector. This change is then replicated to the routing table of all other Exchange servers. If a routing table does not reflect a recent change, it can be rebuilt manually.
NWS	Checking the MTA Queues	Each server creates different queues for all messages awaiting delivery by the MTA. These can be viewed by selecting the **Queues** tab to view the server's queues. Then double-click on the specific queue to get details. Individual messages can be deleted or returned, the message priority can be changed, or detailed message information can be viewed by double clicking on a message.
NWS	MTA Diagnostic Logging	Increasing the diagnostic level of the MTA is useful in troubleshooting MTA problems. View the server's Event Log to see MTA error messages. If you suspect problems with the server's MTA, raise the diagnostics logging level of the MTA. Use the **Diagnostics Logging Property** page to change the level of diagnostics recorded in the server's Application Event Log.
NWS	Maintenance for the Information Store	The Information Store (IS) contains all mailboxes and mail data for the users that have the Exchange server as their home server (Private Information Store), as well as all public folders (Public Information Store) housed on that server.
NWS	Maintenance Schedule for the Information Store	Exchange Server needs information store (IS) maintenance performed periodically, including defragmentation and compacting of the public and private information stores. There are two maintenance modes, online and off-line.

Department	Responsibility	Description
NWS	Online Maintenance	Online maintenance of the IS should be performed on a scheduled basis. This daily, automatic task will compact and defrag the IS. This will slow user response time while the maintenance is running. Therefore, maintenance should be scheduled at the least busy time of the day, usually in the early in the morning. By default, the maintenance is scheduled to run between 1:00am and 6:00am daily.
NWS	Off-line Maintenance	Off-line maintenance must be done by the Exchange administrator. It is similar to online compacting with the exception that it is more time-intensive and requires the information store to be stopped. However, off-line compacting produces better overall performance for the users and is more efficient. Note: Off-line maintenance requires that no users are logged in, since the information store must be stopped. Off-line maintenance should be performed periodically on each Exchange server, but only during scheduled server downtime. Compacting the Exchange databases is done by creating a temporary file (.BAK) into which the records are compressed. This backup file will initially be the same size as the .EDB file being compressed. This means that in order to perform compression, the Exchange Server must have that much free disk space available. An example would be that if the PRIV.EDB private information store is 1.5 GB in size, you must have at lease 1.5 GB free in order to compact the database.
NWS	Maintenance for Exchange Directory	The directory stores all information available regarding an organization's resources and users, such as mailboxes, servers, and folders. Maintaining the directory on each Exchange server includes periodically verifying that the replicated directory information is correct.

Department	Responsibility	Description
NWS	Directory Consistency and Synchronization	If a directory synchronization process is interrupted or you want to make sure that directory synchronization has incorporated the most current information, restart the directory synchronization cycle. This will send a complete list of directory entries to the directory synchronization server, request a full list of entries from the server, and update each server with the most current information. Maintaining a directory on each Exchange server includes periodically verifying that the replicated directory information is correct. Normally, directory replication between servers in the same site is an automatic process in the background and occurs at all times. Replication between sites is a scheduled process that is set up using the Directory Replication connector.
NWS	Initiating Knowledge Consistency Check (KCC)	The administrator can initiate a knowledge consistency check of all directories in the organization if a site or server has a directory that does not reflect all servers in the organization or if there is a suspicion of an error may have occurred during directory replication. Note: This process may take a long time if your organization is large.

9.0 Backup

Since Microsoft Exchange uses Windows NT security for authentication, the Windows NT operating system backup and restore must be taken into consideration, as well as Microsoft Exchange backup and restore. Because of this relationship, Microsoft Exchange disaster recovery cannot be considered independently from Windows NT disaster recovery. Both Exchange and NT must be backed up to allow full recovery. Microsoft Exchange Server was designed so that it does not need to be taken off line to perform a backup. The entire Information Store, Directory, MTA, and System Attendant remain in service during online backup, which includes open files.

9.1. Backup Tape Rotation

Currently, a five-tape rotation is used for the CWS/CMS Exchange environment. A full backup set is performed daily. Monday's tape is taken off-site for safekeeping. Although this method will take the longest amount of time each day, only one tape is required to perform a full restore of the system if there is a catastrophic system failure. It will also recover the Exchange server faster than other backup strategies.

9.2. Online vs. Off-line Backup

9.2.1. Online

Microsoft Exchange online backup requires that the respective service (Information Store, Directory) be running. This backup is performed without disrupting messaging on the Microsoft Exchange-based server. A full online backup, including open files, is the method by which servers are to be backed up on a nightly basis.

9.2.2. Off-Line

This is a file-based backup, with all files closed. This means that no users can be accessing the server during the backup. Since all Microsoft Exchange services must be stopped, this method will interrupt service to the users. Therefore, an off-line backup is not performed unless the server is scheduled for maintenance. This information is included here for comparison only.

9.3. Local vs. Remote Backup/Restore

Not all servers have tape drives installed, so servers without tape drives are backed up remotely from a server with a tape drive. The backup/restore procedure is the same in both cases, except for the location of the data (local or remote).

9.3.1. Local Backup/Restore

Local backup/restore means that the backup is taken with a tape drive physically installed on the server that is being backed up. Local backup/restore operation is independent from the network. It will not increase network traffic during the processing. Each server needs to be touched in order for switching the tapes.

9.3.2. Remote Backup/Restore

Remote backup/restore means the backup is performed over the network; i.e., backing up a server with the tape drive physically installed in another server. The advantage of remote backup/restore is that the backup/restore for all Exchange servers can be operated on a centralized server. It will require that the network function properly. Also, this method will generate network traffic during the backup/restore process.

9.4. Location of Data Files

Exchange data consists of two types of data to be backed up, user data and configuration data. Microsoft Exchange user data is stored in the Information Store (PUB.EDB, PRIV.EDB), PSTs, OSTs, PABs, and transaction logs. Microsoft Exchange configuration data is stored in the Microsoft Exchange Directory (DIR.EDB), the Windows NT Registry, and in various subdirectories under the Microsoft Exchange Server installation path (and possibly paths created after running the Microsoft Exchange Performance Optimizer program).

The actual Microsoft Exchange database files are located in several directories. (See the following table. Note that the default path of *exchsrvr* is shown, but this is selectable by the user during installation.) The transaction logs can be placed on a separate physical disk from the Information Store and Directory files by running the Microsoft Exchange Performance Optimizer program. Reconfiguration of the paths for all the database files can be done using the Database Paths page on the server object.

Data or Information	Directory
Information Store	
Private	*exchsrvr**mdbdata**PRIV.EDB*
Public	*exchsrvr**mdbdata**PUB.EDB*
Directory	*exchsrvr**dsadata**DIR.EDB*
Transaction Logs	
Information Store	*exchsrvr**mdbdata***.LOG*
Directory	*exchsrvr**dsadata***.LOG*

9.5. The Backup Process

To ensure full recovery of a server in case of a system failure, the daily backup process will consist of a daily full online backup.

9.5.1. Steps to Perform On-line Backup

The online backup is run on a daily basis, during a period of low user activity (preferably at night), and backs up the entire server, including the Exchange data stores while the server remains online and available to users.

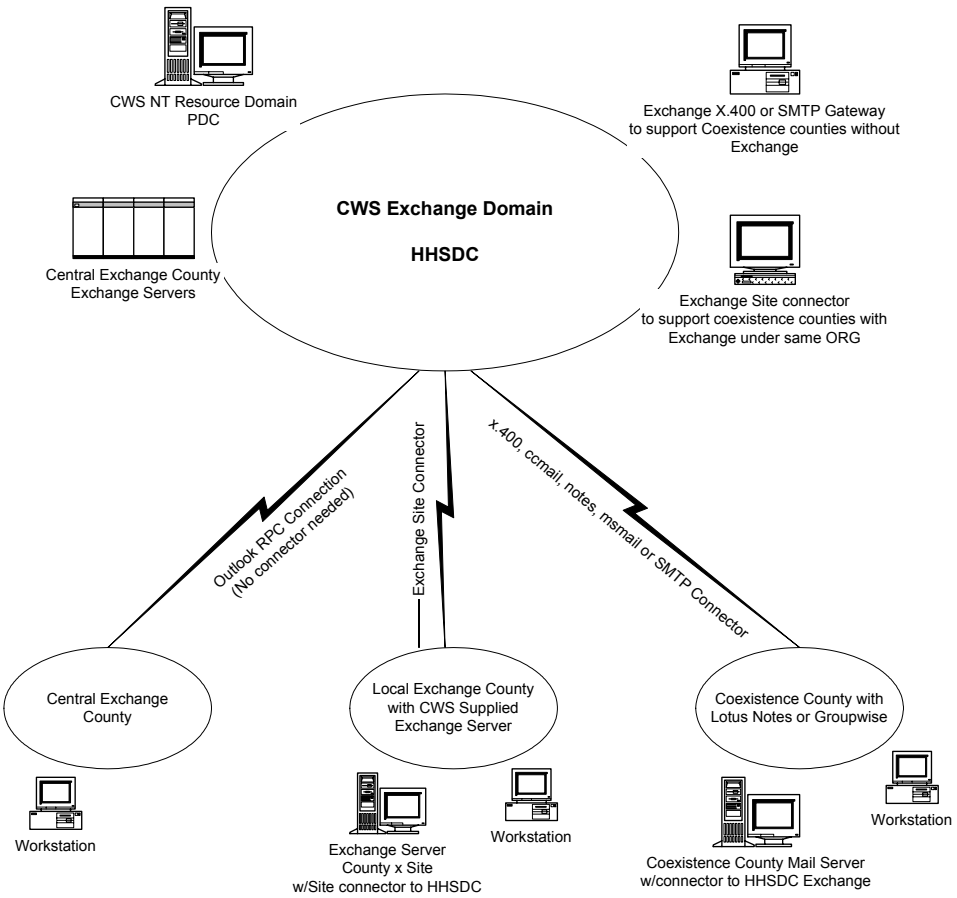
Before the daily online backup can be run, a job must be created that will contain the instructions on what is to be backed up. This step must be performed only once. Once a backup job has been created, it will be scheduled to run every day of the week and must be monitored for successful completion. Also, the tapes must be rotated on a daily basis.

10.0 Site Configuration

This section compares site configuration for locations characterized as “Central Exchange Counties” and “Local Exchange Counties.”

10.1. Central Exchange Counties

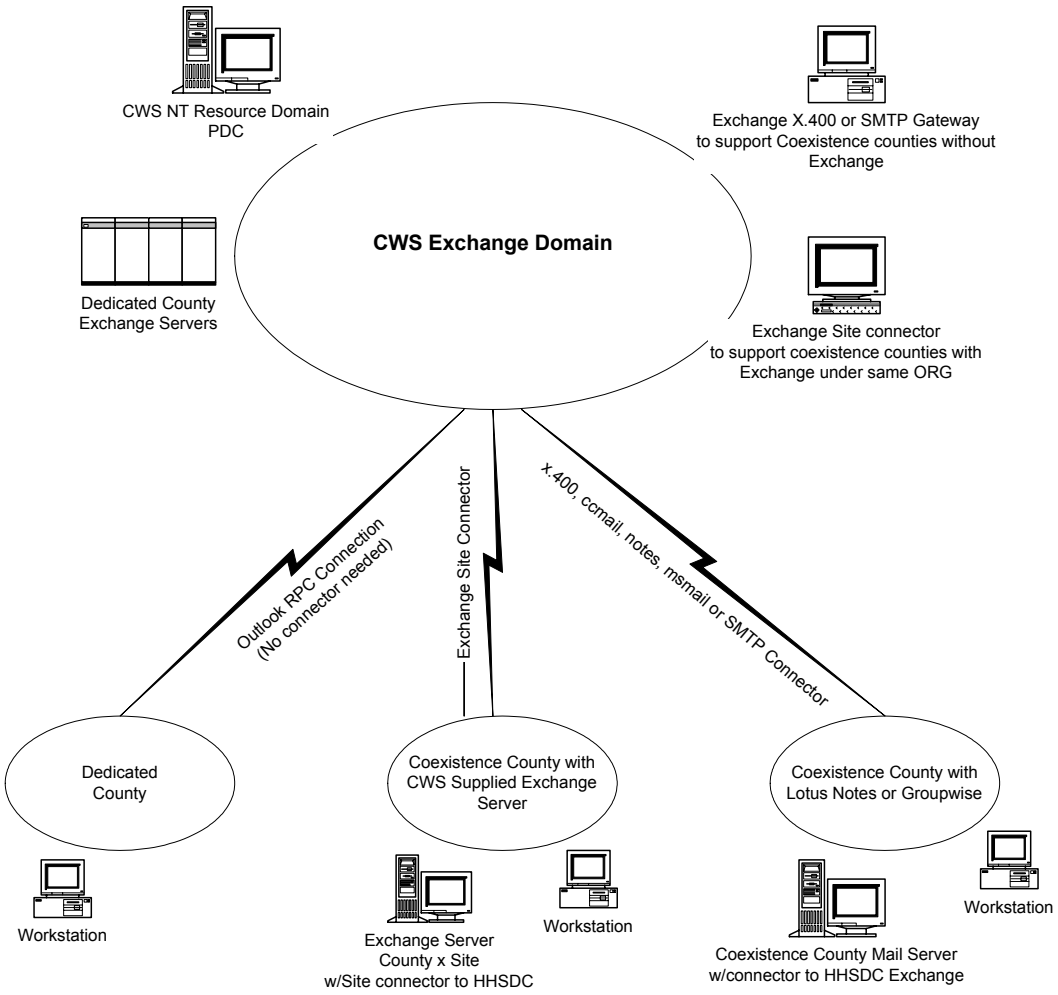
The figure below shows the current Exchange mail system environment. Central Exchange counties are located at a Central Exchange site. The Exchange server is divided into separate containers for each county. Each county will have administrative access to their container only, giving them the ability to add, delete, and modify users and distribution lists at a county level.



10.2. Central Exchange Counties versus Local Exchange Counties

The following figure shows the current Exchange mail system environment. Central Exchange Counties that require their own mail system are fully integrated into the Exchange network by the creation of a separate Exchange site. All other counties are contained within a Central Exchange site.

The Central Exchange site is divided into separate containers for each county. Each county has administrative access only to their container, giving them the ability to add, delete, and modify users and distribution lists at a county level.



11.0 NT Domain Architecture

This section identifies the requirements and architectural design for the Windows NT domain environment.

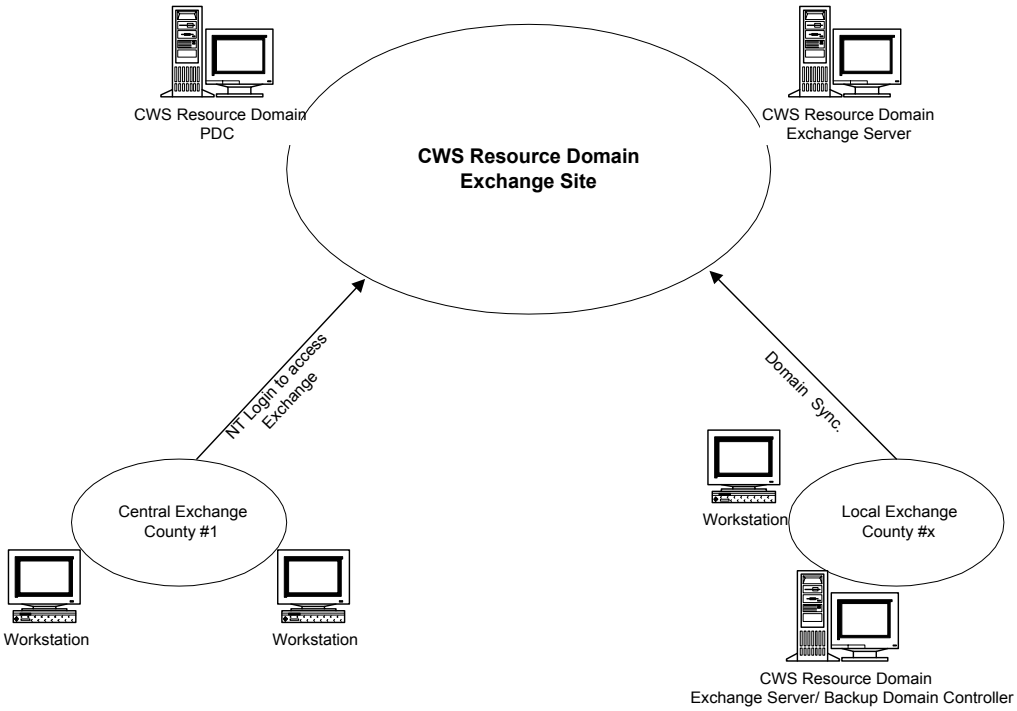
11.1. Requirements

Listed below are the requirements associated with the NT domain architecture in the CWS/CMS operating environment.

- *Support for all CWS/CMS users* - The model must be able to handle enough accounts to accommodate the entire CWS/CMS population 15,000 users.
- *Increase Server Availability* - To be an effective infrastructure component at CWS/CMS, system reliability must be dramatically improved over previous server generations.
- *Support for Remote Users and Remote Access of Resources* - Remote users must be able to access network resources regardless of where they log on within the CWS/CMS NT Network.

11.2. Architectural Design of the CWS/CMS NT Domain Model

Domain structure plays an important part in overall network reliability. Proper planning is essential to maintain a structured network. Once an overall structure has been established, overall network services such as Domain Security, Trust Relationships, WINS, DHCP, and DNS can be administered and managed.



Appendix A

Hardware Configurations

The Exchange server configuration offers an optimal amount of disk fault tolerance and the ability to recover quickly to an operational state should any one drive fail. In such a configuration it is very important to make sure that an NT boot disk is created with an appropriate boot.ini file to be able to start the machine using the alternate disk with the OS on it2. If this is not made, problems can arise in getting a broken mirror set to reboot correctly.

Central Exchange Server Facility

Server 1 : Central Exchange Mailbox Server		
Part No.	***Description***	***Qty.***
8651RH0	Netfinity 7000 Pentium Pro 200-MHz 1024-KB cache Rack Mount	1
94G7147	Pentium Pro 200-MHz 1024-KB cache	3
94G7386	1024 MB (4 x 256 MB) ECC DIMM - 60ns	2
76H3584	PCI ServerRAID II Ultra SCSI Fast/Wide Adapter	2
76H5401	8-MB Battery-Backup Cache	2
86H2432	IBM PCI Etherjet 100/10 Adapter	2
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	8
01K7959	9.1-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	10
35201RU	EXP10 w/Redundant Power	1
94G7150	Redundant Power supply 400w	1
01K8029	IBM PC Server 4.3M External 8mm SCSI	1
	US Robotics Modem V.90	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1

[2] Details of performing this operation are in Windows NT Server Resource Kit, Chapter 6

Server 2 : Central Backup Server		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400mhz 512-KB cache Rack 128-MB RAM	1
01K8023	128-MB ECC DIMM - 60ns	1
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	3
08L3341	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
3447-106	IBM 3447 Digital Linear Tape Library	1
76H5407	Tape Library SCSI Adapter (Required for 3447)	1
	US Robotics Modem V.90	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
	TextPad editor for all NT servers - Enterprise license	1
NTFFAR650EECTC	ArcServe 6.5 for Windows NT (Enterprise License)	1
NTFFD1200EEMTC	ArcServe Disaster Recovery agent 2.0 for WinNT	1
NTFFBA200PEXTC	ArcServe Backup agent for Exchange v. 2.0 for Arcserve 6.5	1
NT-OFA31TC	ArcServe Backup Agent for open files	1
NTFFTA300PECTC	ArcServe Auto Changer	1
	Norton Antivirus	1

Server 3 : Central Exchange IMS Server		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400mhz 512-KB cache Rack 128-MB RAM	1
10L5884	Pentium II 400-MHz 512 cache	1
01K8023	128 MB ECC DIMM - 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	8
08L3341	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
	Norton Antivirus V7	1

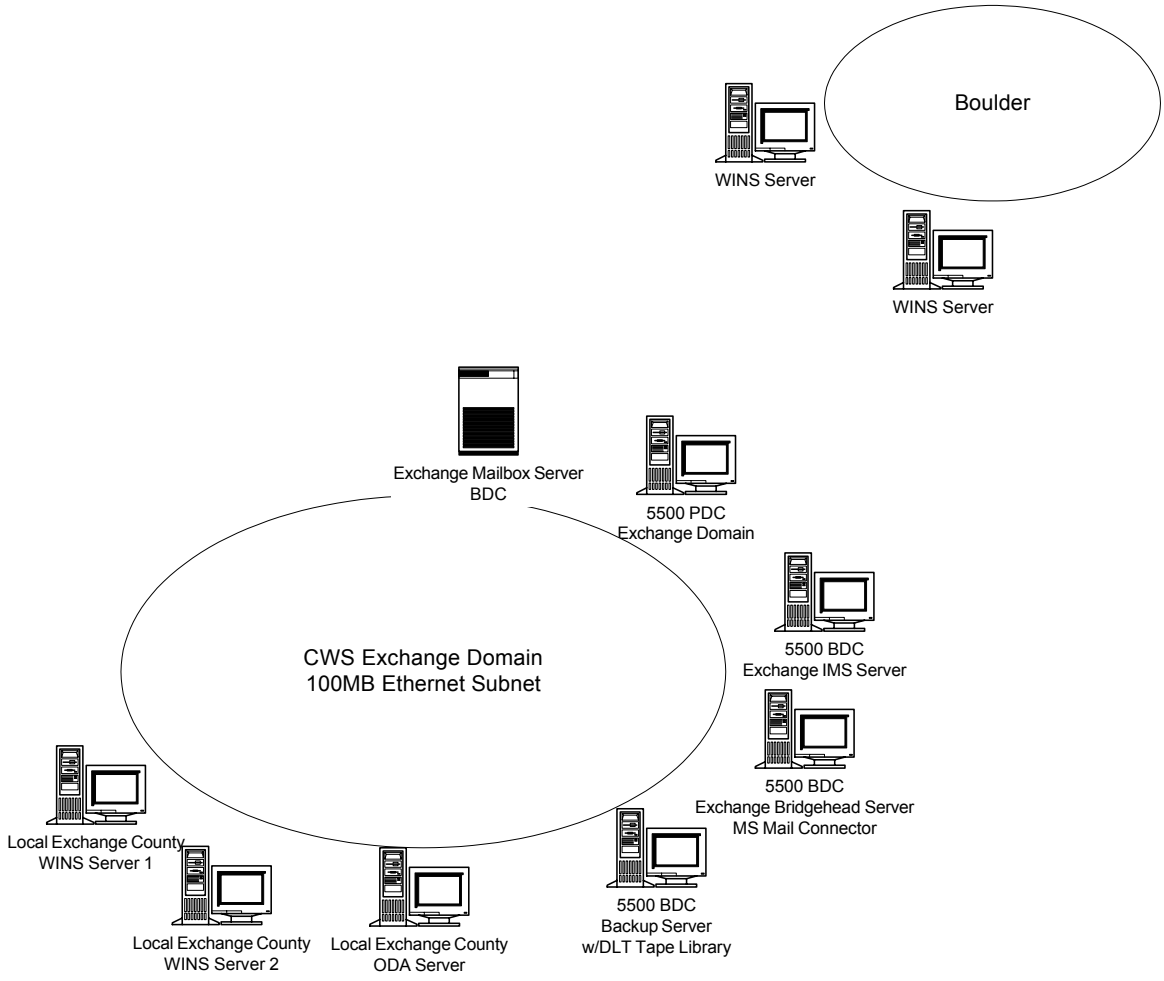
Server 4 : Central WINS Server 1		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400-MHz 512-KB cache Rack 128-MB RAM	1
10L5884	Pentium II 400mhz 512 cache	1
01K8023	128-MB ECC DIMM - 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	3
08L3341	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1
	Norton Antivirus V7	1

Server 5 : Central WINS Server 2		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400-MHz 512-KB cache Rack 128mb Ram	1
10L5884	Pentium II 400-MHz 512 cache	1
01K8023	128-MB ECC DIMM – 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	3
08L3341	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1

Server 6 : Central CWS Mail PDC		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400-MHz 512-KB cache Rack 128-MB RAM	1
10L5884	Pentium II 400-MHz 512 cache	1
01K8023	128-MB ECC DIMM - 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	4
08L3341	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1

Server 7 : Central Exchange Bridgehead Server		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400-MHz 512-KB cache Rack 128-MB RAM	1
10L5884	Pentium II 400-MHz 512 cache	1
01K8023	128-MB ECC DIMM - 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	8
86H2432	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
	Norton Antivirus V7	1

Server 8 : Central CWS ODA Transaction Server		
Part No.	***Description***	***Qty.***
8660-4RU	Netfinity 5500 Pentium II 400-MHz 512-KB cache Rack 128-MB RAM	1
10L5884	Pentium II 400-MHz 512 cache	1
01K8023	128-MB ECC DIMM - 60ns	3
01K8009	4.51-GB Wide Ultra SCSI SCA-2 Hot Swappable HDD 10,000	4
86H2432	Netfinity 10/100 Ethernet Adapter	2
01K8026	Netfinity 400w Redundant Power Supply	1
2273275-V40VL	NT Server 4.0 Standard License	1
2272075V40VL	NT Server 4.0 Client Access License	118
	NT Transaction Server (included with NT 4.0 Option Pack)	1
	NT 4.0 Option Pack	1
	Norton Antivirus V7	1



Local Exchange Server Facility

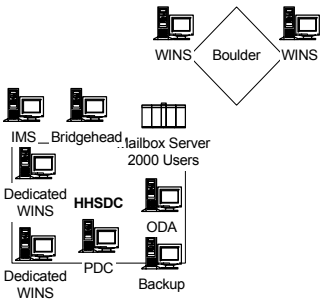
Local Exchange Servers Counties

Hardware Configuration

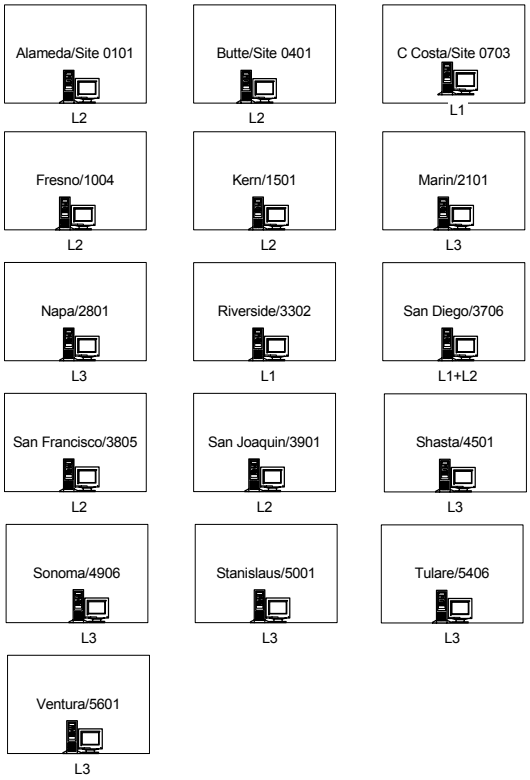
L1 Server – 250 Users		
Part. No.	***Description***	***Qty.***
8660-41U	IBM Netfinity 5500, PII-400-MHz, 512-KB L2 cache, 128-MB ECC DIMM, 32X CD-ROM, 10/100 Ethernet port, 4 drop SCSI 68 pin cable, Video port, Audio port, Diskette Drive, Mouse, Keyboard	1
01K8009	4.51-GB Ultra SCSI Wide SCA-2 Hot Swap HDD 10,000	2
08L3341 41H8900	IBM Netfinity 10/100 Ethernet Adapter or IBM PCI Token Ring Adapter	1
6546-40N	IBM G51 Monitor	1
94G6674	APC Smart-UPS 1400	1
01K1320	IBM 20/40 DLT SCSI Tape Drive	1
AP9605 AP9604	SNMP Module for UPS (Ethernet) or SNMP Module for UPS (Token Ring) or	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
NTFFAR650SEWTC	ArcServe 6.5 for Windows NT (license)	1
NTFFD1200EEMTC	ArcServe Disaster Recovery agent 2.0 for WinNT	1
NTFFBA200PEXTC	ArcServe Backup agent for Exchange v. 2.0 for Arcserve 6.5	1
NT-OFA31TC	ArcServe Backup Agent for open files	1
	Norton Antivirus V7	

L2 Server – 500 Users		
Part. No.	***Description***	***Qty.***
8660-41U	IBM Netfinity 5500, PII-400-MHz, 512-KB L2 cache, 128-MB ECC DIMM, 32X CD-ROM, 10/100 Ethernet port, 4 drop SCSI 68 pin cable, Video port, Audio port, Diskette Drive, Mouse, Keyboard	1
10L5884	Pentium II 400-MHz 512-KB cache	1
01K8023	128-MB ECC DIMM - 60ns	2
01K8009	4.51-GB Ultra SCSI Wide SCA-2 Hot Swap HDD 10,000	2
01K8054	9.1-GB wide ultra SCSI SCA-2 Hot Swap HDD 10,000	3
08L3341 41H8900	IBM Netfinity 10/100 Ethernet Adapter or IBM PCI Token Ring Adapter	2 or 1
654640N	IBM G51 Monitor	1
94G6674	APC Smart-UPS 1400	1
01K1320	IBM 20/40 DLT SCSI Tape Drive	1
AP9605 AP9604	SNMP Module for UPS (Ethernet) or SNMP Module for UPS (Token Ring)	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
NTFFAR650SEWTC	ArcServe 6.5 for Windows NT (license)	1
NTFFD1200EEMTC	ArcServe Disaster Recovery agent 2.0 for WinNT	1
NTFFBA200PEXTC	ArcServe Backup agent for Exchange v. 2.0 for Arcserve 6.5	1
NT-OFA31TC	ArcServe Backup Agent for open files	1
	Norton Antivirus V7	1

L3 Server – 750 users		
Part. No.	***Description***	***Qty.***
8660-41U	IBM Netfinity 5500, PII-400-MHz, 512-KB L2 cache, 128-MB ECC DIMM, 32X CD-ROM, 10/100 Ethernet port, 4 drop SCSI 68 pin cable, Video port, Audio port, Diskette Drive, Mouse, Keyboard	1
10L5884	Pentium II 400-MHz 512-KB cache	1
01K8023	128-MB ECC DIMM - 60ns	3
01K8009	4.51-GB Ultra SCSI Wide SCA-2 Hot Swap HDD 10,000	2
01K8054	9.1-GB wide ultra SCSI SCA-2 Hot Swap HDD 10,000	4
08L3341 41H8900	IBM Netfinity 10/100 Ethernet Adapter or IBM PCI Token Ring Adapter	2 or 1
654640N	IBM G51 Monitor	1
01K8026	Netfinity 400W Redundant Power Supply	1
94G6674	APC Smart-UPS 1400	1
01K1320	IBM 20/40 DLT SCSI Tape Drive	1
AP9605 AP9604	SNMP Module for UPS (Ethernet) or SNMP Module for UPS (Token Ring) or	1
2273275-V40VL	NT Server 4.0 Standard License	1
312-00805	NT Exchange v5.5 (Enterprise) competitive upgrade package	1
NTFFAR650SEWTC	ArcServe 6.5 for Windows NT (license)	1
NTFFD1200EEMTC	ArcServe Disaster Recovery agent 2.0 for WinNT	1
NTFFBA200PEXTC	ArcServe Backup agent for Exchange v. 2.0 for Arcserve 6.5	1
NT-OFA31TC	ArcServe Backup Agent for open files	1
	Norton Antivirus V7	1



Counties using Central Exchange:
Alpine, Amador, Calaveras, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Imperial, Inyo, Kings, Lake, Lassen, Madera, Mariposa, Mendocino, Modoc, Mono, Monterey, Nevada, Placer, Plumas, San Benito, San Luis Obispo, Shasta, Sierra, Siskiyou, Sutter, Tehama, Trinity, Tulare, Tuolume, Yolo, Yuba.



Exchange Server Placement

Appendix B

Outlook Client Requirements

User Requirements

- *Compatibility.* The deployment of Microsoft Outlook Client can not adversely affect any other applications running on their desktop
- *Performance.* The performance of Microsoft Outlook Client must be the same as or better than that of the previous system

Deployment Requirements

- *Automation.* Must be able to automate the installation process to effectively install the client software on a large number of desktops
- *Customization.* Must be able to preset defaults during the installation process
- *Automatic updates.* Must be able to update the client automatically

Administrative/Operations Requirements

- *Troubleshooting.* Must have the ability to troubleshoot connectivity between the client and Microsoft Exchange Server

Appendix C

Listing of Acronyms

CWS/CMS	Child Welfare Services / Case Management System
DEA	Domain Enterprise Administration
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DS	Directory Structure
EDSS	Enterprise Directory Synchronization System
HHSDC	Health and Human Services Data Center
GAL	Global Address List
GB	Gigabyte (1024 Megabytes)
HD	Help Desk
IMS	Internet Mail Service
IP	Internet Protocol
IS	Information Store
KB	Kilobyte (1024 Bytes)
Kbps	Kilobits per second
KCC	Knowledge Consistency Check
LAN	Local Area Network
MB	Megabyte (1024 Kilobytes)
Mbps	Million Bits Per Second
MTA	Message Transfer Agent
NOS	Network Operating System
NWS	NetWorkStation Management
OST	Off-line Folder Storage
PPP	Point-to-Point Protocol
PSS	Product Support Services

PST	Personal Folder Storage
RACF	Resource Access Control Facility
SMTP	Simple Mail Transport Protocol
SOC	State of California
TCP/IP	Transmit Control Protocol / Internet Protocol
WAN	Wide Area Network
WINS	Windows Internet Naming Service

Appendix D

Performance Testing

Microsoft Exchange Server was analyzed for network traffic performance capacity and scalability. A testing utility called LoadSim was used to emulate typical mail client-server interaction when a user retrieves and sends mail to the mail server under test using MAPI protocols. The analysis used a load model that is typical of a CWS/CMS, medium-activity mail load.

Methodology

When conducting complex experiments, good methodology is essential. Use the following methodology with Load Simulator to produce reliable results:

- **Goal** - To determine network bandwidth needs based on historical data of the current CWS/CMS mail system.
- **Network Topology** - Every effort was made to ensure lab experiments conditions matched the production environment. Line speed simulators were used to duplicate the bandwidth the production network.
- **Actual Usage May Vary** - The behavior of real users is seldom identical to the behavior of test users. Therefore, assumptions were made based on a medium corporate email user.

Background

Load Simulator

Load Simulator allows for testing how your messaging server computer performs under different message loads. You can define specific workloads in Load Simulator to exercise servers in a controlled manner. This lets you accurately study server behavior under specific conditions. You can use this information to help determine the optimum number of users per server, pinpoint performance bottlenecks, and evaluate server hardware performance.

Load Simulator can be used in the following ways:

- To test the capacity and compare server hardware performance
- To determine network bandwidth requirements given different user behaviors
- To perform tuning exercises such as making configuration changes and seeing how they affect performance without affecting real users

Load Simulator is a multi-client emulator program that allows you to carry out large-scale experiments without configuring a large group of client machines. When the user would be taking some action, Load Simulator sends messages to the server instead of an actual client. The Microsoft Exchange Client module has been developed to mimic as closely as possible the calls that the Microsoft Outlook clients would make.

Load Simulator allows you to create models of user behavior and server topology. You can specify the following attributes:

- The number of times per day a user sends a new message
- How often the user reads messages
- What percentage of messages are deleted, saved in folders, or forwarded to others
- The number of servers in your topology
- The number of users assigned to each server
- What client modules are being used

As Load Simulator runs a scenario, user activities are generated based on the probability of the model you provide. For example, if the model says that users send 14.6 messages in an eight-hour day, Load Simulator will generate messages for each user in the scenario at an average rate of 1.82 messages per hour, though the intervals between messages will not be uniform. Random variations are included because real users vary their activities considerably.

A Load Simulator scenario emulates client requests; although this is only one part of capacity planning. The following information is not provided by Load Simulator and is critical to capacity planning decisions:

- *The behavior characteristics or user profile of your users*. Each user population is unique and will place different demands on the messaging server. Only research and live monitoring can tell you how CWS/CMS users differ from Load Simulator's light, medium, and heavy profiles.
- *The storage capacity required by users*. A server computer provides disk storage for each user it hosts. If you are using online backup, you need to double this requirement so an equal quantity of free disk space exists for each user.
- *The amount of time required to back up your server*. The length of time required to back up a server is directly related to user storage quotas and the speed of your backup hardware. Most deployments require backups to run and finish overnight.
- *The performance impact of certain client features on the Microsoft Exchange Server*. Load Simulator does not emulate Inbox Assistant rules or Outlook's preview view.

Canonical User Profiles

There are certain user behaviors that are consistent regardless of what messaging client is being used. For example, a user sends a certain number of messages per day. This number may vary from person to person according to the user's business needs, but does not change from one messaging client to another.

Below are some canonical user definitions illustrating a simple way of characterizing user loads. These are called light, medium, and heavy users. A medium user is defined as one who sends 14 messages per day regardless of the type of client. This load is a combination of newly composed messages and replies to and forwards of received messages. The frequency of

tasks performed and number of messages and folders created during initialization vary according to the canonical profile.

These profiles provide a common set of loads that can be used for comparison purposes. Load Simulator has three canonical user profiles.

Task or Condition	Light User	Medium User	Heavy User
Send Mail	2	4	6
Process Inbox	12	12	12
Browse Mail	5	15	20
Schedule+	1	5	10
Number of Messages in Inbox	1	4	9
Number of Messages in Deleted Items Folder	1	1	1
Number of New Folders (5 Messages per New Folder)	20	40	60

Test Profiles

All tests were performed using the Microsoft medium user profile. A network packet analyzer was used to record network utilization and monitor TCP/IP port usage. IP port usage was monitored to determine if Exchange conformed to CWS/CMS security standards. The following port usage was observed and remains a requirement for all tests performed. Server: 135, 1042, 1044, 1048, 1049, 1311 and up, 2308 and up. Workstation: 1311 and up. This port usage is similar to ftp in that each new process requested by the client spawns a new port. Exchange uses port 135 to make RPC (remote procedure calls) and ports 1024 to 4000 for client requests. This port usage currently conforms with HHSDC's standard router configuration and should not pose a problem.

Test #1 (20 Users)

Time	3:37:54
Total Frames	20k
Total Bytes	7.98MB
Average Frames /second	2
Average Bytes /second	610
Average Utilization	0.05% (10-MB Ethernet)
Peak Utilization	3.00% (20 users logging in 10 seconds)

Test #2 (65 Users)

Time	1:58:30
Total Frames	38.13k
Total Bytes	11.09MB
Average Frames /second	5
Average Bytes /second	1559
Average Utilization	0.12 % (10-MB Ethernet)
Peak Utilization	3.18% (65 users logging in 20 seconds)

Test #3 (100 Users)

Time	15:24:34
Total Frames	443.93k
Total Bytes	211.80MB
Average Frames /second	8
Average Bytes /second	3.818
Average Utilization	0.31% (10-MB Ethernet)
Peak Utilization	4.35% (95 users logging in 45 seconds)

Results summary

Microsoft provided the LoadSim tools for Exchange e-mail load simulation. The medium MAPI user canonical profile was chosen reflecting the workload of a typical CWS/CMS e-mail environment. Acceptable performance for this test is an average response time of less than two seconds for clients.

Bandwidth usage based on a 10-MB Ethernet segment for 100 users in test #3 shows .31% average utilization which on a T1 circuit would be divided roughly by 10, equating to about 3.10% usage to support 100 users. The peak usage of 4.35% would translate to 43.5%. 100 users logging in all within one minute generating this peak utilization of 43.5%. This situation is highly unlikely in a production environment and was only used to provide testing data.